# MODELO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA FISCALÍA DE LA CIUDAD DE NEIVA-HUILA

**ANDRÉS FELIPE PERDOMO ALVARADO**

**UNIVERSIDAD COOPERATIVA DE COLOMBIA**
**FACULTAD DE INGENIERÍAS**
**PROGRAMA INGENIERÍA DE SISTEMAS**
**NEIVA**
**2016**

# MODELO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA FISCALÍA DE LA CIUDAD DE NEIVA-HUILA


**ANDRÉS FELIPE PERDOMO ALVARADO**

**Informe final de seminario de profundización presentado para optar al título de INGENIERO DE SISTEMAS**

**Asesor**
**PhD. MATEO LEZCANO**

**UNIVERSIDAD COOPERATIVA DE COLOMBIA**
**FACULTAD DE INGENIERÍAS**
**PROGRAMA INGENIERÍA DE SISTEMAS**
**NEIVA**
**2016**

**NOTA DE ACEPTACIÓN**

**Presidente del Jurado**

**Jurado**

**Jurado**

Neiva, Junio de 2016

## DEDICATORIA

A Dios por darnos la vida y fortaleza para escalar un peldaño más en nuestras vidas.

A nuestros familiares y amigos por su apoyo incondicional a lo largo de la carrera.

**CONTENIDO**

**Pág.**

## LISTA DE FIGURAS

**Pág.**

## RESUMEN

El presente proyecto tiene como propósito diseñar un conjunto de políticas de seguridad de la información para la fiscalía de la ciudad de Neiva. La fase inicial está dirigida a la investigación y análisis de las amenazas presentes en la entidad, así como los posibles riesgos de seguridad; se examinarán las normas implementadas y la manera en que deben potenciarse a través de: buenas prácticas, nuevas herramientas y normas de seguridad.

Durante la fase final, se tendrá un catálogo de normas, que una vez implementadas en la organización, permitirá aumentar los niveles de seguridad, dando una solución eficaz ante las posibles amenazas que puedan afectar la información. Permitiendo así que en la fiscalía se pueda llevar a cabo un manejo organizado de la información que sea altamente seguro.

# INTRODUCCIÓN

Las tecnologías de la información y la comunicación (TIC) han avanzado de una manera sorprendente, día a día aparecen nuevos equipos con capacidad de hardware superior, a un tamaño y precio reducido, lo que facilita acceder a estas tecnologías sin realizar grandes inversiones.

En la actualidad, prácticamente todas las empresas utilizan las TIC para optimizar sus procesos laborales, permitiendo ejecutar y procesar la información de manera más fácil y rápida, convirtiéndola en un activo importante de la empresa, y por consiguiente en un blanco de ataque. Por eso y debido a las posibles amenazas que se puedan presentar, es fundamental garantizar la seguridad de la información, con un conjunto de estándares y buenas prácticas, para asegurar la integridad, confidencialidad y disponibilidad, tanto interna como externa. Pues el impacto de una amenaza materializada no solo puede producir daño o alteración de la información, sino que puede generar consecuencias aún mayores, como: pérdidas materiales y/o económicas, problemas legales, mala reputación de la organización, afectación de la imagen pública o incluso poner en riesgo su continuidad en el mercado.

El enfoque de este proyecto, va dirigido a la propuesta de un conjunto de políticas de seguridad que establecerán normas para realizar un manejo adecuado de la información por medio de: hardware, software, controles, procedimientos, estándares y capacitaciones; que deberán organizarse y seguir determinados lineamientos para poder combatir las amenazas, reducir al mínimo los posibles daños y garantizar la prosperidad laboral de la entidad.

# 1. PLANTEAMIENTO DEL PROBLEMA

“La fiscalía es una entidad de la rama judicial del poder público con plena autonomía administrativa y presupuestal, cuya función está orientada a brindar a los ciudadanos una administración de justicia cumplida y eficaz” (Fiscalía General de la Nación, 2016), es por ello que tales entidades deben tener un estricto grado de seguridad que permita proteger su infraestructura y la información que se maneje.

El estudio que se presenta en este trabajo se llevó a cabo en la fiscalía de la ciudad de Neiva, en ella no están establecidos los niveles de seguridad apropiados.

Una de las principales causas que pone en riesgo la información, es el factor humano y en gran parte por falta de sensibilización, pues las personas no son conscientes de lo importante que es garantizar la seguridad de la información que manejan.

Actualmente en la institución no se tiene control al suministrar información, pues entregan las contraseñas de usuarios administradores a personal que ni siquiera pertenecen a la organización. De igual manera la mayoría de los usuarios ponen sus contraseñas al alcance de cualquier individuo por no memorizarlas, o porque son poco robustas y predecibles, lo cual facilita las posibilidades de hurto de información.

Otro importante factor de riesgo se encuentra en el manejo o administración de las cuentas de usuario, debido a que se crean cuentas para personas que solo van a laborar por un tiempo determinado y estas siguen en funcionamiento aun después de haberse culminado ese lapso. También la falta de control de permisos, ya que en algunos casos se les asignan usuarios a otras personas para no tener que crear un usuario nuevo, pero no se modifican los permisos que este posee, por consiguiente no se tiene en cuenta el daño que puede ocasionar un usuario con más permisos de los necesarios.

## 2. JUSTIFICACIÓN

Algunas empresas ven la implementación de políticas de seguridad como una opción pero en realidad la adopción de tales políticas es una necesidad impostergable de cualquier entidad. Es por esto que las normas buscan disminuir las brechas que se puedan presentar, las cuales pueden ser aprovechadas por hackers y/o empleados para efectuar robo, destrucción, modificación o manipulación inadecuada de la información entre otras.

Con base en lo anterior se realiza este proyecto, planteando soluciones a las problemáticas ya expuestas, con la ayuda de procedimientos, políticas y formación de talento humano, para garantizar así la seguridad de la información y haciendo de ella un recurso más confiable, evitando situaciones de peligro.

# 3. OBJETIVOS

## 3.1 OBJETIVO GENERAL

Diseñar un conjunto de políticas de seguridad de la información para la fiscalía de la ciudad de Neiva, en base a la norma ISO/IEC 27001:2013.

## 3.2 OBJETIVOS ESPECÍFICOS

- Analizar los riegos y vulnerabilidades que se presentan en la entidad, tanto a nivel de talento humano, como en los sistemas de información y de cómputo.

- Analizar las políticas de seguridad que se encuentran implementadas.

- Elaborar un grupo de reglas organizacionales para el uso adecuado del hardware y software, que permitan proteger la confidencialidad, integridad y disponibilidad de la información.

# 4. ESTADO DEL ARTE

La seguridad de la información tiene un origen lejano, que se remonta a la época en que se crearon los primeros mensajes cifrados, los cuales tenían el objetivo de asegurar que la información fuera confidencial. Con el paso del tiempo, la seguridad se convirtió en un tema sumamente relevante para las empresas, por lo cual se vuelve necesaria la implementación de las políticas de seguridad. Estas políticas lo que hacen es permitir a la entidad prevenir, proteger y manejar los riesgos para evitar que puedan materializarse en daños y afectar el desarrollo normal de la organización.

## 4.1 ÁMBITO LOCAL Y DEPARTAMENTAL

A través de técnicas de levantamiento de información, como entrevistas y encuestas realizadas al personal del área de tecnologías de la información (TI), de la fiscalía de la ciudad de Neiva Huila, se pudo concluir que actualmente la entidad no tiene implementado un sistema de políticas de seguridad de la información, por lo cual no realizan un manejo adecuado de esta y la mayor parte del tiempo se encuentra vulnerable.

Actualmente a nivel local no se cuenta con empresas certificadas en seguridad de la información, pero existen muchas organizaciones que se rigen bajo estándares y normas básicas de seguridad, implementadas por la misma entidad a fin de proteger la información producida.

## 4.2 ÁMBITO NACIONAL E INTERNACIONAL

Según la organización internacional de normalización (ISO[1]), actualmente Colombia cuenta con aproximadamente ochenta empresas con certificación válida de la norma ISO IEC 27001:2013, con un incremento anual de aproximadamente del 2% (The ISO Survey, 2015).Pero que hoy día gracias a la evolución de las tecnologías de la información y la comunicación, se tiene a disposición las herramientas en línea y plantillas prefabricadas, que le facilitan a las organizaciones el poder conocer más acerca de esta norma y lograr una implementación y certificación de la misma, sin realizar grandes inversiones económicas, y sin necesidad de contratar auditores ni personal externo, de manera que en los siguientes años la tasa de certificación será mayor a la actual.

Según la encuesta anual realizada por la organización internacional de normalización, presentada en el año 2015, durante el año 2014 se expidieron

[1] http://www.iso.org/iso/home.htm, sitio web de la organización internacional de normalización.

23.972 certificados de la norma ISO 27001, con un aumento del 7% en comparación con el año anterior (The ISO Survey Executive summary 2014, 2015). Es posible apreciar que cada vez son más las organizaciones y personas certificadas en esta norma y la importancia que tiene la ISO 27001 en las empresas, que además de garantizar la seguridad de la información, también ayuda en gran medida al mejoramiento de la producción, pues una empresa organizada es más eficiente y competitiva.

# 5. MARCO CONCEPTUAL

## 5.1 SEGURIDAD INFORMÁTICA

“La seguridad informática es un conjunto de métodos y herramientas destinados a proteger la información y por ende los sistemas informáticos ante cualquier amenaza, un proceso en el cual participan personas” (Ramió, 2006). Su propósito es garantizar la confidencialidad, integridad y disponibilidad de la información evitando que la misma pueda ser alterada, borrada o falsificada.

Los métodos y herramientas pueden ser: políticas, procesos, controles, organización, hardware, software y comportamiento ético por parte del personal, entre otros.

## 5.2 CONCEPTOS DE SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información hace referencia a la seguridad de los activos en forma general, incluyendo la seguridad informática, seguridad de las tecnologías de la información y la comunicación y la seguridad de los datos. A continuación se definen algunos conceptos relevantes en cuanto a esta temática.

- SGSI: Siglas de sistema de gestión de seguridad de la información.
- Usuario: Persona, entidad, grupo de trabajo o empleado.
- Confidencialidad: Asegurar que la información pueda ser accedida únicamente por los usuarios permitidos.
- Integridad: Propiedad de la información, donde se pretende que la información almacenada no pueda ser modificada sin permiso.
- Disponibilidad: Los usuarios con autorización, deben tener siempre acceso a la información.
- Activo: Son los recursos con los que una organización cuenta, tales como: computadores, manuales, documentación física y digital, software, personal humano, memorias USB, entre otros. Los activos en sí, constituyen la empresa.
- Amenaza: Cualquier circunstancia potencial que pueda causar daño o perdidas a los activos.

- Vulnerabilidad: Debilidad de un activo que puede permitir que una amenaza se materialice.

- Probabilidad: Posibilidad de que una amenaza aproveche la vulnerabilidad para materializar el riesgo.

- Riesgo: Posibilidad de que una amenaza se materialice.

- Riesgo residual: Nivel restante del riesgo, después de ser tratado.

- Identificación del riesgo: Proceso para encontrar, enumerar y caracterizar los elementos de un riesgo, que afecte la seguridad de la información.

- Evitar riesgo: Decisión de una organización cuando no quiere afrontar una situación de riesgo o decide retirarse de esta.

- Transferencia del riesgo: Compartir con otra organización las consecuencias negativas de un riesgo.

- Ataque: Una acción que pueda explotar una vulnerabilidad.

- Impacto: Consecuencia que se presenta sobre un activo, una vez que se ha materializado una amenaza.

- Control o salvaguarda: práctica, mecanismo o procedimiento que reduce los niveles de riesgo.

- La dirección: Es la encargada de llevar a cabo los objetivos de la organización y desarrollar los planes a largo plazo. Está compuesta por la presidencia y los directivos.

- Nube (Cloud computing): Conjunto de servicios y datos almacenados en servidores o computadores, que se encuentran conectados entre sí, y que se puede hacer uso de ellos al acceder al internet.

## 5.3 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

El sistema de gestión de seguridad de la información, es una herramienta de la norma ISO 27001:2013, que tiene como objetivo ayudar en la gestión de las entidades u organizaciones. Se realiza identificando principalmente los riesgos, para posteriormente ser analizados, evaluados y minimizados, todo de una forma documentada y sistematizada, que es dada a conocer a la organización.

El SGSI incorpora un modelo PDCA[2] (Planificar, hacer, medir, actuar) como método de mejora continua.

Figura 1. Modelo PDCA de la norma ISO 27001


Fuente: tomado de http://siempresa.blogspot.com.co/2012/07/sgsi-sistemas-de-gestion-de-la.html

El objetivo del PDCA, como se aprecia en la figura 1, es garantizar la implementación y funcionamiento del SGSI a través de un ciclo de mejora continua, a fin de tener la información lo más segura posible a través del tiempo y de las nuevas problemáticas que aparecen con él.

## 5.4 ESTABLECER EL SGSI

Establecer o planificar el SGSI es la etapa inicial y principal para la implementación de la ISO 27001:2013 en cualquier entidad. En esta etapa se definirá el alcance, las políticas, procedimientos, procesos y objetivos del sistema, de acuerdo a los riesgos que posea la empresa.

**5.4.1 Alcance del SGSI.** Esta es la primera fase para la planificación del SGSI, aquí se deben dejar en claro las áreas o dependencias de la entidad, en donde se implementará principalmente y en cuáles se hará posteriormente. La definición del alcance se efectúa con un análisis de las características del negocio, organización, activos, cantidad de empleados, número de sedes, áreas, información manejada, tecnología, procesos, sistemas y todo lo que pueda verse afectado por el SGSI.

[2] PDCA, por sus siglas en inglés: Plan (Planificar), Do (Hacer), Check (Medir), Act (Actuar).

**5.4.2 Política de seguridad.** Documento en el cual se estipulan las políticas de seguridad y en donde se puede apreciar el compromiso por parte de la dirección, al revisar y aprobar dichas políticas. También se observa el enfoque que tiene la organización, respecto a la gestión de la seguridad de la información.

**5.4.3 Análisis y Evaluación de riesgos.** El análisis y evaluación se hace con base en los activos definidos por el alcance del SGSI, en caso de que la organización tenga demasiados activos, se centralizará en los más críticos o fundamentales para la entidad.

El objetivo de este proceso es identificar y evaluar los riesgos a los cuales están expuestos los activos, para poder definir las probabilidades e impactos de estos y así mismo seleccionar los controles más apropiados para la seguridad de la información, manteniendo los riesgos en un nivel aceptable de impacto.

Figura 2. Metodología de análisis y evaluación de riesgos.


Fuente: El autor.

El proceso de análisis y evaluación se desarrolla a través de la implementación de una metodología, como se aprecia en la figura 2, la cual se basa en las buenas prácticas recomendadas por la norma ISO 27001:2013, esta contiene los pasos que se deben llevar a cabo, desde identificar el riesgo, hasta los controles a implementar para mitigarlo o eliminarlo.

**5.4.4 Objetivos de control para el tratamiento de riesgos.** Los objetivos de control y controles para el tratamiento de riesgos, se seleccionan con base en la evaluación de riesgos. Dependiendo del impacto y de la probabilidad, se identifica el control más apropiado para tratar cada riesgo.

**5.4.5 Plan de Tratamiento de riesgos.** Documento genérico que se obtiene del análisis de activos, recursos disponibles, evaluación de riesgos y la selección de los objetivos de control y controles. En el plan de tratamiento de riesgos se identifican las acciones, responsabilidades, prioridades y recursos necesarios para que la dirección pueda llevar a cabo una gestión adecuada de la seguridad de la información. Como resultado, los riesgos identificados deben ser tratados con la implementación de controles apropiados, evitados en caso de que la organización no quiera afrontar el riesgo o ser transferidos a otras organizaciones siempre y cuando esta acción sea más viable que tratar internamente el riesgo, como ejemplo se puede citar el caso de adquirir seguros para los activos, comprar servicios de almacenamiento en la nube para archivos o copias de seguridad, entre otros.

**5.4.6 Formación y toma de conciencia.** La formación y toma de conciencia es uno de los elementos fundamentales para una implementación exitosa del SGSI. Para esto, la dirección debe comprobar que todo el personal humano que tenga deberes relacionados con el SGSI, esté lo suficientemente capacitado para llevar a cabo estas tareas de forma adecuada. Para comprobar lo anterior, la dirección debe:

- Especificar las competencias que deberá tener el personal para efectuar las tareas del SGSI.
- Satisfacer esas necesidades a través de formación o de contratación de talento humano ya capacitado.
- Evaluar la eficacia al realizar las tareas.
- Llevar registros de estudios, formación, habilidades, experiencia y cualificación.

Adicional a esto, la dirección tiene que asegurar que todo el personal relevante para la implementación del SGSI, sepa de la importancia que tiene realizar sus actividades de seguridad de la información.

## 6. CRONOGRAMA DE ACTIVIDADES

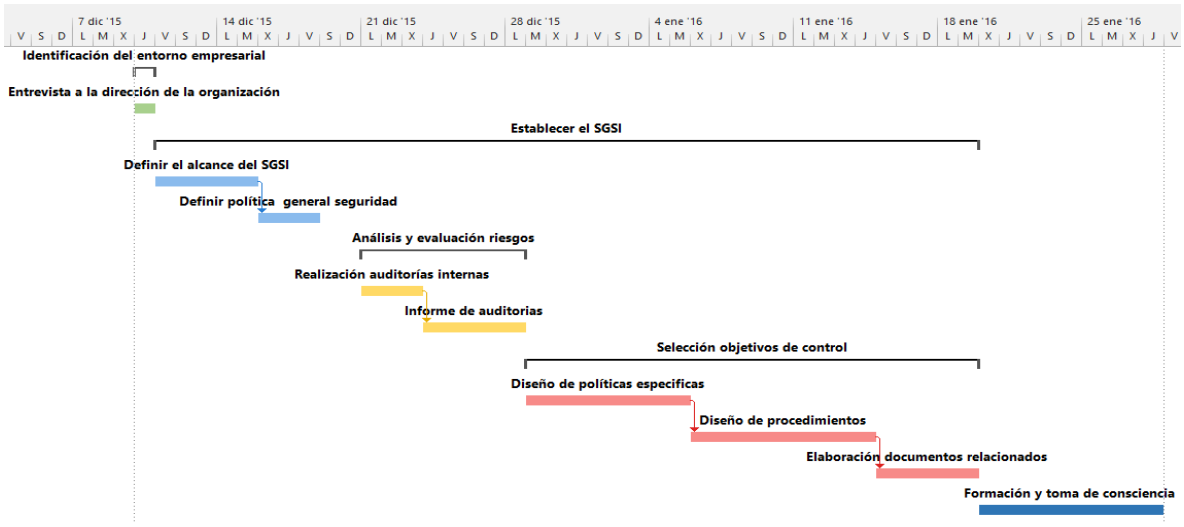
En las figuras 3 y 4 se encuentra el cronograma de actividades del proyecto, donde se observan las actividades que se van a realizar y el tiempo dedicado a cada una de ellas.

Figura 3. Cronograma de actividades

| Nombre de tarea | Duración | Comienzo | Fin |
|---|---|---|---|
| **1 Identificación del entorno empresarial** | **1 día** | **jue 10/12/15** | **jue 10/12/15** |
| 1.1 Entrevista a la dirección de la organización | 1 día | jue 10/12/15 | jue 10/12/15 |
| **2 Establecer el SGSI** | **27 días** | **vie 11/12/15** | **mar 19/01/16** |
| 2.1 Definir el alcance del SGSI | 3 días | vie 11/12/15 | mar 15/12/15 |
| 2.2 Definir política general seguridad | 3 días | mié 16/12/15 | vie 18/12/15 |
| **2.3 Análisis y evaluación riesgos** | **6 días** | **lun 21/12/15** | **lun 28/12/15** |
| 2.3.1 Realización auditorías internas | 3 días | lun 21/12/15 | mié 23/12/15 |
| 2.3.2 Informe de auditorias | 3 días | jue 24/12/15 | lun 28/12/15 |
| **2.4 Selección objetivos de control** | **15 días** | **mar 29/12/15** | **mar 19/01/16** |
| 2.4.1 Diseño de políticas especificas | 5 días | mar 29/12/15 | mar 5/01/16 |
| 2.4.2 Diseño de procedimientos | 7 días | mié 6/01/16 | jue 14/01/16 |
| 2.4.3 Elaboración documentos relacionados | 3 días | vie 15/01/16 | mar 19/01/16 |
| **3 Formación y toma de consciencia** | **7 días** | **mié 20/01/16** | **jue 28/01/16** |

Fuente: El autor.

Figura 4: Línea de tiempo




Fuente: El autor.

El proyecto se compone de tres tareas o actividades principales que a su vez están compuestas por sub tareas. Las tareas principales son: identificación del entorno empresarial, establecer el SGSI y formación y toma de consciencia.

Cada actividad se efectuara en un determinado número de días y solo se empezará a desarrollar la siguiente actividad, cuando la anterior se encuentre totalmente concluida.

# 7. PRESUPUESTO

Tabla 1. Presupuesto

| PRESUPUESTO | | | | | | |
|---|---|---|---|---|---|---|
| **Tipo** | **N°** | **Descripción** | **Unidad** | **Cantidad** | **Valor Unitario** | **Valor Total** |
| **Talento Humano** | 1 | Identificación entorno empresarial | Hora | 8 | $ 23.000,00 | $ 184.000,00 |
| | 2 | Definir alcance del SGSI | Hora | 24 | $ 23.000,00 | $ 552.000,00 |
| | 3 | Definir política general de seguridad | Hora | 24 | $ 23.000,00 | $ 552.000,00 |
| | 4 | Análisis y evaluación de riesgos | Hora | 48 | $ 23.000,00 | $ 1.104.000,00 |
| | 5 | Seleccionar objetivos de control | Hora | 120 | $ 23.000,00 | $ 2.760.000,00 |
| | 6 | Formación y toma de conciencia | Hora | 56 | $ 23.000,00 | $ 1.288.000,00 |
| **Recursos técnicos** | 7 | Norma NTC-ISO/IEC 27001 | Docum. | 1 | $ 45.000,00 | $ 45.000,00 |
| | 8 | Computador portátil Dell Inspiron (Procesador: AMD quad core A8, memoria RAM: 8GB, Disco duro: 1 TB) | Unidad | 1 | $ 1.350.000,00 | $ 1.350.000,00 |
| | 9 | Impresora multifuncional HP 2545 | Unidad | 1 | $ 400.000,00 | $ 400.000,00 |
| | 10 | Papel | Resma | 2 | $ 12.300,00 | $ 24.600,00 |
| | | | | | **Total Gastos** | $ 8.214.600,00 |

Fuente: El autor.

En la tabla 1 se aprecia el presupuesto general para el desarrollo del proyecto, el cual tiene un costo general de 8.214.600 COP[3]. Este se divide en dos partes:

- Talento humano: El personal laborara a un precio de 23.000 COP la hora y se invertirán un total de doscientas ochenta horas (280) para concluir con las actividades descritas en el cronograma de actividades del proyecto.

- Recursos técnicos: Aquí se especifican todos los equipos, documentos, materiales y herramientas necesarias para que el talento humano pueda iniciar y culminar las actividades.

[3] COP: Signo representativo del peso colombiano.

# 8. POLÍTICAS DE SEGURIDAD INFORMÁTICA (PSI)

Las políticas de seguridad informática se dividen en un conjunto de artículos, que a su vez se subdividen en: políticas de seguridad organizativa, políticas de seguridad física, políticas de seguridad lógica, plan de contingencia, capacitación del personal y actualización de las políticas de seguridad. Estos artículos explican las responsabilidades del personal de la organización para el manejo adecuado la información y cómo deberán reaccionar ante las posibles amenazas. También se define la importancia de los activos y las áreas o personal que están asignados a ellos.

## 8.1 POLÍTICAS DE SEGURIDAD ORGANIZATIVA

**Art. 1.** Toda la información, activos y servicios de red, son exclusivos del personal organizativo de la fiscalía, cualquier modificación en las normativas será adecuada como política.

**Art. 2.** La alta gerencia nombrará un comité de seguridad, el cual se encargará de verificar que se esté cumpliendo con las normativas, al mismo tiempo se encargará de:

- Confirmar el cumplimiento de las políticas.
- Aplicar sanciones.
- Elaborar planes de seguridad.
- Crear planes de contingencia.
- Mantener al talento humano capacitado.
- Estar pendiente de cualquier anomalía o sugerencia que ameriten mejorar la seguridad de la información.
- Mantener siempre a la alta gerencia informada sobre la seguridad.

Este comité estará conformado por:
- Gerente.
- Jefe de sistemas.
- Administrador de red.

**Art. 3.** El área de tecnologías de la información (área de TI o ATI) será la encargada de velar por la confidencialidad, integridad y disponibilidad de la información.

## 8.2 POLÍTICAS DE SEGURIDAD FÍSICA

### 8.2.1 Acceso Físico

**Art. 1**. La organización establecerá un área donde se ubicarán los servidores y sistemas de telecomunicación.

**Art. 2.** Los servidores y sistemas de comunicación deberán estar protegidos físicamente, para que los usuarios no tengan acceso a estos.

**Art. 3.** Solo se podrá acceder a áreas restringidas, en acompañamiento del jefe o el responsable de esa área.

**Art. 4.** Cualquier persona, empleado o contratista que ingrese a la fiscalía, deberá registrarse al ingresar o salir de las instalaciones, también se deberá dejar registro de cualquier equipo o herramientas que vayan a ingresar.

### 82.1 Equipos

**Art. 1.** El área TI deberá tener un control de los equipos y licenciamientos.

**Art. 2.** El área de TI se encargará de programar los mantenimientos correctivos y preventivos que se realizarán a los equipos.

**Art. 3.** Los mantenimientos a los equipos, solo podrán ser ejecutados por personal de TI o por contratistas con la debida autorización del jefe de TI.

**Art. 4.** El área de talento humano deberá notificar al área de TI, cuando un usuario no labore más en la organización, para retirarles las credenciales de acceso a los equipos.

**Art. 5.** La protección física de los equipos, será responsabilidad del usuario o persona a la que se le asignó.

**Art. 6.** Los usuarios deberán comunicar de forma inmediata al área de TI cuando se identifique cualquier riesgo real o potencial sobre los equipos.

**Art. 7.** Los equipos pertenecientes a las distintas oficinas, estarán ubicados en sitios estratégicos, libres de humedad y posibles riesgos físicos.

**Art. 8.** Los usuarios no podrán mover los equipos, ni instalar o remover dispositivos o activos de su área de trabajo.

**Art. 9.** Todos los equipos estarán etiquetados y ordenados para llevar el debido control sobre ellos.

## 8.3 POLÍTICAS DE SEGURIDAD LÓGICA

**Art.1.** Es responsabilidad de los usuarios mantener segura la información almacenada en los distintos equipos o dispositivos de almacenamiento.

### 8.3.1 Adquisición de software

**Art. 1.** Los usuarios no podrán instalar software alguno a ninguno de los equipos, servidores, computadores o cualquier dispositivo que se encuentre conectado a la red de la organización.

**Art. 2.** Si un usuario requiere la instalación de un software en específico, deberá justificar esa necesidad al área de TI para que ellos la analicen y hagan la debida instalación de la aplicación.

**Art. 3.** La compra de cualquier licencia de software deberá ser aprobada por el jefe de TI.

**Art. 4.** El área de TI llevará inventario de todas las licencias instaladas en los equipos de la entidad.

**Art. 5.** Los usuarios deberán reportar al área de TI, si encuentran instaladas aplicaciones sin licencias, software no autorizado por la empresa o software con licenciamiento ilegal o pirata.

### 8.3.2 Red

**Art. 1.** El objetivo de la red es el de intercambiar información internamente entre usuarios, oficinas, departamentos, y externamente entre usuarios con empresas prestadoras de servicios, contratistas, proveedores y demás entidades que tengan relación con la fiscalía.

**Art. 2.** Cada usuario es responsable de la información que solicite o envíe por la red.

**Art. 3.** Los usuarios pueden ver, crear, modificar o borrar información de un equipo, solo con el consentimiento de la persona que tiene asignado ese equipo.

**Art. 4.** Solo se permitirá el uso de servicios de red que sean fundamentales para el desarrollo de la empresa. Estos servicios son autorizados por el área de TI.

**Art. 5**. Las contraseñas de acceso a los sistemas, equipos o servicios son de uso personal y no pueden ser transferidas a otros usuarios o terceros.

### 8.3.3 Servidores

**Art. 1.** Cualquier instalación o modificación que se le haga a los servidores es responsabilidad del área de TI.

**Art. 2.** El área de TI se encargará de administrar y limitar los archivos, servicios, recursos, programas y permisos a los cuales tendrán acceso los usuarios.

**Art. 3.** El área de TI deberá llevar un monitoreo y control del funcionamiento del servidor.

**Art. 4**. El servidor deberá funcionar las 24 horas del día, los 365 días del año.

**Art. 5.** ATI realizará dos mantenimientos preventivos al año, para garantizar el funcionamiento del servidor.

**Art. 6.** La información crítica del servidor se respaldará diariamente.

**Art. 7.** Los documentos web serán respaldados semanalmente.

**Art. 8.** La configuración del servidor se respaldará mensualmente.

**Art. 9.** El servidor solo proveerá servicios autorizados previamente por el área de TI.

### 8.3.4 Correo Electrónico

**Art. 1.** El área de TI es la encargada de suministrar las cuentas y contraseñas de acceso a los usuarios.

**Art. 2**. El usuario deberá cambiar la contraseña que se le asignó cuando ingrese por primera vez al correo.

**Art. 3.** La contraseña de acceso deberá ser mayor o igual a ocho caracteres, incluyendo como mínimo un carácter numérico y uno especial.

**Art. 4.** Los usuarios no deberán utilizar cuentas que estén asignadas a otros empleados.

**Art. 5.** Cualquier información recibida por correo electrónico es considerada propiedad de la fiscalía y por consiguiente es responsabilidad de los usuarios velar por la seguridad de la misma.

### 8.3.5 Seguridad de Cómputo

**Art. 1.** El área de TI se encargará de proporcionar el mayor nivel de seguridad posible a los equipos, todo esto a través de la implementación de herramientas, antivirus, firewalls y servicios.

**Art. 2.** ATI podrá monitorear el tráfico de red, para identificar posibles fallos o uso indebido de la red.

### 8.3.6 Usuarios de acceso

**Art. 1.** Todo el personal perteneciente a la fiscalía dispondrá de un nombre de usuario y contraseña para acceder a los sistemas de información o la red. Siempre y cuando su labor a desempeñar lo amerite.

**Art. 2.** La contraseña de usuario estará compuesta como mínimo de ocho caracteres, los cuales deberán incluir caracteres numéricos y especiales.

**Art. 3.** La contraseña es de carácter privado y cada usuario es responsable de ello.

**Art. 4.** Cada usuario es responsable de la información que se crea, modifica o borra de su equipo asignado.

**Art. 5.** El personal contratista o que trabajará temporalmente, se le asignará una cuenta de usuario y contraseña la cual será desactivada una vez que culmine el contrato o prestación de servicios.

**Art. 6.** Los usuarios deberán informar al área de TI ante cualquier anomalía que presencien en los equipos o en la red.

**Art. 7.** Las cuentas pueden ser suspendidas, si el usuario hace un uso indebido de los equipos, servicios de red o viola alguna política de seguridad establecida.

**Art. 8.** Los usuarios deberán bloquear siempre los equipos con contraseña, cuando no se encuentren presentes en el escritorio.

### 8.3.7 Antivirus

**Art. 1.** Todos los equipos de cómputo deberán disponer de un antivirus y un anti espía, que será implementado por el área de TI.

**Art. 2.** Los usuarios deberán analizar los dispositivos de almacenamiento extraíble como memorias USB, tarjetas SD y unidades de disco duro portátiles, antes de abrir cualquier archivo para identificar posibles virus y eliminarlos.

**Art. 3.** En caso de que un virus no pueda ser eliminado o enviado a cuarentena, el área de TI deberá aislar el equipo de la red, hasta que se dé una solución.

**Art. 4.** Los usuarios no deberán desinstalar el antivirus de los equipos.

**Art. 5.** El antivirus debe actualizarse de forma automática desde la base de datos de virus cada ocho horas.

**Art. 6.** Cualquier inconveniente que tenga el usuario con el antivirus, deberá comunicárselo al área de TI.

### 8.4 PLAN DE CONTINGENCIA

**Art. 1.** Tener soporte tanto físico como magnético de la información de manera que se pueda recuperar en caso de pérdida.

**Art. 2.** Realizar copias de seguridad de la información en la nube.

**Art. 3.** Realizar y tener una copia de seguridad física, en un lugar distinto a la fiscalía para prever perdidas.

**Art. 4.** Elaborar manuales con los respectivos procedimientos y operaciones a seguir en caso de una contingencia.

**Art. 5.** Realizar pruebas de funcionalidad al plan de contingencia.

**Art. 6.** Realizar revisiones y modificaciones al plan de contingencia.

### 8.5 CAPACITACIÓN DEL PERSONAL

**Art. 1.** Todo empleado nuevo en la fiscalía, deberá ser instruido y capacitado sobre las políticas y normativas de seguridad implementadas a la fecha en la organización.

### 8.6 ACTUALIZACIÓN DE LAS POLÍTICAS DE SEGURIDAD

**Art. 1.** Todas las políticas y normas descritas en este documento, están sujetas a cambios y modificaciones. Para que una política pueda ser modificada, deberá primero ser analizada y aprobada por el comité de seguridad.

**Art. 2.** Cada seis meses se deberá realizar una reunión del comité para realizar las debidas modificaciones a las normativas de seguridad.

**Art. 3.** El comité tendrá como responsabilidad divulgar a los jefes de área cualquier modificación realizada a las normas.

**Art. 4.** Si un usuario o empleado no tiene conocimiento de las normativas, esto no lo exonera de sanciones en caso de que incumpla con alguna política.

# 9. CONCLUSIONES

- Con la investigación realizada, se puede concluir que muy pocas organizaciones a nivel regional y nacional, implementan políticas de seguridad de la información, muchas de ellas no lo ven como una necesidad o beneficio, mientras que otras implementan algunas normas, pero no concientizan al personal o se preocupan de que estas normas sigan en funcionamiento.

- No tener implementado un conjunto de políticas, hace que las organizaciones terminen gastando más dinero del que gastarían certificándose en una norma de seguridad de la información, comprando herramientas y aplicaciones costosas que no dan solución en gran medida a las problemáticas que se presentan y sin saber que hoy día, es más fácil certificarse, gracias a las herramientas en línea que pueden encontrar en la internet.

- El objetivo de implementar normas de seguridad, es el de proteger la información, garantizar su integridad, confidencialidad y disponibilidad, capacitar al personal humano y hacerle ver la importancia que este tiene en la aplicación de las políticas de seguridad, permitiendo a las organizaciones desenvolverse mejor en el mercado, frente a otras entidades que no poseen normas de seguridad.

- En el trabajo presentado se realizó un análisis de riegos y vulnerabilidades presentes en la Fiscalía de la ciudad de Neiva y se determinó que no existían políticas de seguridad adecuadas.

- Tomando en cuenta la conclusión anterior se diseñó un conjunto de políticas de seguridad de la información que se basan en la norma ISO/IEC 27001:2013.

## BIBLIOGRAFÍA


Academy, 2. (2005). 27001 Academy. Obtenido de http://www.iso27001standard.com/es/que-es-iso-27001/

Borau, P. (31 de Julio de 2012). SGSI: SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. Obtenido de http://siempresa.blogspot.com.co/2012/07/sgsi-sistemas-de-gestion-de-la.html

Cigras. (2014). Implementación efectiva de un SGSI ISO 27001. Obtenido de http://www.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014%20-%20Exposici%C3%B3n%202%20CIGRAS%20ISO%2027001%20-%20rbq.pdf

Costas, S. J. (2011). Seguridad informática. Bogotá: Bogotá : Ra-Ma : Ediciones de la U, 2011.

Fiscalía General de la Nación. (2016). Obtenido de http://www.fiscalia.gov.co/colombia/

Gómez Vieites, Á. (2013). Auditoría de seguridad informática. Bogotá: Bogotá : Ediciones de la U ; Madrid : StarBook Editorial, 2013.

Group, B. (2014). Sistema de gestión ISO/IEC 27001 de Seguridad de la Información. Obtenido de http://www.bsigroup.com/es-ES/Seguridad-de-la-Informacion-ISOIEC-27001/

Mintic. (s.f.). Obtenido de http://www.mintic.gov.co/gestionti/615/w3-article-5482.html

Ramió, J. (2006). Libro electrónico de seguridad informática y criptografía, versión 4.1.

Seguridad de la información y protección de datos. (s.f.). Obtenido de https://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion/

Standardization, I. O. (2014). ISO. Obtenido de http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certificate=ISO/IEC%2027001&countrycode=CO#countrypick
The ISO Survey. (2015). Obtenido de http://www.iso.org/iso/iso_survey_executive-summary.pdf?v2014

The ISO Survey Executive summary. (2015). Obtenido de ISO: http://www.iso.org/iso/iso_survey_executive-summary.pdf?v2014